Some Properties of Certain Finite Algebras.[*]

By Edward Kircher.

The object of this paper is to study some of the properties of a finite algebra $\mathfrak{A}$ whose elements combine by addition and multiplication, subject to the commutative, associative, and distributive laws. The elements also form a group when combined by addition, so that subtraction is always possible in $\mathfrak{A}$, but division, the inverse of multiplication, is not always possible and when possible is not necessarily unique. The unit element of the additive group we denote by 0. We also assume the existence of a *unit* U in $\mathfrak{A}$, *i. e.*, an element such that the equation $UX=0$ in $\mathfrak{A}$ admits only the solution $X=0$. Division by a unit is always possible in $\mathfrak{A}$ and is uniquely determined.[†] Again $\mathfrak{A}$ contains a sub-algebra of elements simply isomorphic to the set of integers $0, 1, \ldots, m-1$, taken modulo m.[‡] The elements in $\mathfrak{A}$ corresponding to 0 and 1 are denoted by these symbols. Papers closely related to the subject in hand have been written by Vandiver,[†] Dickson,[§] and Fraenkel.[||] The last of these papers has many results analogous to those of the following pages, but restricts itself to algebras $\mathfrak{A}$ all of whose elements satisfy the unique factorization law.

I. *The Finite Algebra $\mathfrak{A}$ As a System of Residue Classes.*

In a previous paper[¶] the writer discussed the group properties of the residue classes belonging to a modular system $\mathfrak{M}=(\mathfrak{m}_n, \ldots, \mathfrak{m}_1, \mathfrak{m})$, where $\mathfrak{m}$ is an ideal of the algebraic field Ω of degree k, while

$$\mathfrak{m}_i=(\psi_1^{(i)}, \ldots, \psi_j^{(i)}, \ldots, \psi_{j_i}^{(i)}),$$

where each $\psi_j^{(i)}$ is a rational integral function of x_i with coefficients that are in turn rational integral functions of $x_1, x_2, \ldots, x_{i-1}$, with coefficients

[*] Presented to the American Mathematical Society, December 27, 1915.

[†] H. S. Vandiver, *Transactions of the American Mathematical Society*, Vol. XIII (1912), pp. 293–304.

[‡] L. E. Dickson, "Linear Groups," p. 9.

[§] L. E. Dickson, *Transactions of the American Mathematical Society*, Vol. VI (1905), pp. 344–348.

[||] A. Fraenkel, "Ueber die Teiler der Null und die Zerlegung von Ringen," *Crelle's Journal*, Vol. CXLV (1915), pp. 139–175.

[¶] Kircher, "Group Properties of the Residue Classes of Certain Kronecker Modular Systems," etc., *Transactions of the American Mathematical Society*, Vol. XVI (1915), pp. 413–434. This reference will be cited as K in the following pages.

that are integers in Ω. We assume the number of residue classes to be finite, which is always true if the following conditions are fulfilled:

(a) Every $\psi_j^{(i)}$ is of finite degree in x_i;

(b) Every $\mathfrak{m}_i$ contains at least one $\psi_j^{(i)}$ whose highest power of x_i has a coefficient α relatively prime to the modular system

$(\mathfrak{m}_{i-1}, \mathfrak{m}_{i-2}, \ldots., \mathfrak{m}_1, \mathfrak{m})$, *i. e.*, $(\alpha, \mathfrak{m}_{i-1}, \mathfrak{m}_{i-2}, \ldots., \mathfrak{m}_1, \mathfrak{m}) = (1)$.*

(c) For all values of i we have $j_i > 0$ and finite.

The residue classes are formed by all rational integral functions in $x_1, \ldots., x_n$, with coefficients that are integers in Ω, taken modulo $\mathfrak{M}$. Such a set of residue classes evidently forms a finite algebra of the type under consideration. We shall now show that every finite algebra $\mathfrak{A}$ satisfying the conditions laid down can be represented by the residue classes of a modular system $\mathfrak{M}$. The existence and proof of this correspondence was first brought to the writer's attention by H. S. Vandiver.

We know that $\mathfrak{A}$ contains a sub-algebra of integral marks which we may denote by $0, 1, \ldots., m-1$. If there exists another element x_1 of $\mathfrak{A}$ not contained in the above set, it follows that $\mathfrak{A}$ contains the marks

$$\alpha_0 x_1^r + \alpha_1 x_1^{r-1} + \ldots. + \alpha_r,$$

where the α's range over $0, 1, 2, \ldots., m-1$. Since $\mathfrak{A}$ is finite it follows that in the set $x_1, x_1^2, \ldots., x_1^k, \ldots.$ there must exist an element x_1^k such that there exists a relation of the type $x_1^k = \beta_1 x_1^{k-1} + \beta_2 x_1^{k-2} + \ldots. + \beta_k$, which can be written in the form

$$x_1^k + \gamma_1 x_1^{k-1} + \gamma_2 x_1^{k-2} + \ldots. + \gamma_k = 0, \qquad \beta_i = -\gamma_i, \tag{I}$$

where the γ's are integral marks. Let k be the smallest integer for which a power of x_1 will satisfy a relation of this type. Then all polynomials in x_1 are included in the set $\beta_1 x_1^{k-1} + \beta_2 x_1^{k-2} + \ldots. + \beta_k$, the β's being integral marks. This does not preclude the existence of relations of lower degree between the powers of x_1 provided the coefficient of the highest power of x_1 in this relation is not prime to m. Such a relation is of the form

$$\delta_1 x_1^{k-t} + \delta_2 x_1^{k-t-1} + \ldots. + \delta_{k-t} = 0. \tag{II}$$

For brevity denote relation (I) by $\psi_1^{(1)}$, and the various relations (II) by $\psi_2^{(1)}, \ldots., \psi_j^{(1)}, \ldots., \psi_{j_1}^{(1)}$. If there exists in $\mathfrak{A}$ another element x_2 that cannot be written as a polynomial in x_1 alone, we can show in a similar manner that all elements of $\mathfrak{A}$ that can be obtained from x_1, x_2, and the integral marks, are of the form $\varepsilon_1 x_2^t + \varepsilon_2 x_2^{t-1} + \ldots. + \varepsilon_t$, where the ε's range over all distinct elements of the form $\beta_1 x_1^{k-1} + \beta_2 x_1^{k-2} + \ldots. + \beta_k$. Similarly, there exists a relation

*K, see theorem, p. 425.

$\psi_1^{(2)} = x_2^m + \sigma_1 x_2^{m-1} + \ldots\ldots + \sigma_m = 0$, and possibly some relations of lower degree in x_2 which we may designate by $\psi_2^{(2)}, \ldots\ldots, \psi_{j_2}^{(2)}$. The coefficients of the highest powers of x_2 in these last relations are not relatively prime to the modular system $(\psi_1^{(1)}, \ldots\ldots, \psi_j^{(1)}, \ldots\ldots, \psi_{j_1}^{(1)}, m)$. This process may be repeated until all elements of $\mathfrak{A}$ have been exhausted. By referring to a theorem previously proved * we see that the totality of relations $\psi_j^{(i)} = 0$ so obtained together with $m = 0$ defines a modular system whose residue classes correspond to the elements of $\mathfrak{A}$. We therefore have the

THEOREM: *The elements of the finite algebra* $\mathfrak{A}$ *may be represented by the residue classes of a modular system* $\mathfrak{M} = (\mathfrak{m}_n, \mathfrak{m}_{n-1}, \ldots\ldots, \mathfrak{m}_i, \ldots\ldots, \mathfrak{m}_1, \mathfrak{m})$, *where m is a rational integer and* $\mathfrak{m}_i = (\psi_1^{(i)}, \ldots\ldots, \psi_j^{(i)}, \ldots\ldots, \psi_{j_i}^{(i)})$, *where each* $\psi_j^{(i)}$ *is a rational integral function of* $x_1, x_2, \ldots\ldots, x_i$ *with coefficients that are rational integers, at least one* $\psi_j^{(i)}$ *in each* $\mathfrak{m}_i$ *having a term of form* $x_i^{\alpha_i}$ *representing the highest power of* x_i *in that* $\psi_j^{(i)}$.

We are now able to study the properties of the abstract elements of our algebra by studying the concrete residue classes of a modular system representing that algebra. This fact will often prove to be of help in the following pages.

For the necessary definitions and properties of modular systems we refer the reader to the reference *K* previously cited.† There he will find the definition of such terms as: $\mathfrak{M}$ contains the modular system $\mathfrak{M}'$, $\mathfrak{M}$ is divisible by $\mathfrak{M}'$, $\mathfrak{M}$ is an irreducible, an absolute prime, or a simple system. In Fraenkel's paper the term $\mathfrak{M}$ contains $\mathfrak{M}'$ is the same as $\mathfrak{M}$ is divisible by $\mathfrak{M}'$.

Let the elements of $\mathfrak{A}$ be represented by the residue classes of a modular system $\mathfrak{M}$ in the domain of integrity of $(1, x_1 \ldots\ldots, x_n)$. If δ and ϵ are any two polynomials ın this domain and C_δ and C_ϵ are the residue classes containing them, then the operations of addition, subtraction, and multiplication in $\mathfrak{A}$ are evidently defined by the relations:

$$C_\delta + C_\epsilon = C_{\delta+\epsilon}, \qquad C_\delta - C_\epsilon = C_{\delta-\epsilon}, \qquad C_\delta C_\epsilon = C_{\delta\epsilon}.$$

In general, the letters A, B, C, etc., denote elements of $\mathfrak{A}$, but units are often denoted by U. The significance of 1 and 0 has already been explained. We say that A is *divisible* by B if there exists an element C in $\mathfrak{A}$ such that $A = BC$. From the definition of a unit it follows that the product of a U into each element of $\mathfrak{A}$ gives back all elements of $\mathfrak{A}$, and therefore, by a theorem previously proved,‡ we have the modular system $(U, \mathfrak{M}) = (1)$, *i. e.*, a unit of $\mathfrak{A}$ is *relatively prime* to $\mathfrak{M}$. Two elements of $\mathfrak{A}$ that differ from another by a unit factor only are said to be *equivalent* and for purposes of factorization will be regarded as essentially the same. We write $A \equiv 0$, mod $\mathfrak{M}'$, if every

* K, p. 425.

† K, pp. 415–418.

‡ K, pp. 431–432.

polynomial ξ in the residue class A of the system $\mathfrak{M}$ satisfies the relation $\xi\equiv 0$, mod $\mathfrak{M}'$. In particular, if $A\equiv 0$, mod $\mathfrak{M}$, we have $A=0$ in $\mathfrak{A}$. This also defines the meaning of $A\equiv B$, mod $\mathfrak{M}'$. Since $(U, \mathfrak{M})=(1)$ it follows that $\mathfrak{M}$ contains no system $\mathfrak{M}'$ such that $U\equiv 0$, mod $\mathfrak{M}'$, where U is any unit of $\mathfrak{A}$. When $\mathfrak{M}$ is an absolute prime modular system the algebra $\mathfrak{A}$ reduces to a Galois field as studied by E. H. Moore and Dickson.*

II. *The Standard Forms of Elements in* $\mathfrak{A}$.

It has previously been proved† that we have:

THEOREM: *If* $\mathfrak{M}=\prod\limits_{i=s}^{i=1}\mathfrak{Q}_i$, *where the* $\mathfrak{Q}_i$ *are the simple factors of* $\mathfrak{M}$, *and if* f_i, $i=1, 2, \ldots, s$, *are any polynomials in* $x_1, x_2, \ldots, x_n$, *with rational integral coefficients, then there exist polynomials* f *such that* $f\equiv f_i$, *mod* $\mathfrak{Q}_i$, $i=1, 2, \ldots, s$, *and these polynomials are all congruent each to each modulo* $\mathfrak{M}$.

The different polynomials f of this theorem evidently form a residue class of $\mathfrak{M}$ and represent an element A of $\mathfrak{A}$. If $\mathfrak{M}=\mathfrak{Q}_1\mathfrak{Q}_2\ldots\mathfrak{Q}_i\ldots\mathfrak{Q}_s$ represents $\mathfrak{M}$ factored into its simple modular factors we shall say that A_i is a *simple* element of type i in $\mathfrak{A}$ if every polynomial ξ in the residue class representing A_i, mod $\mathfrak{M}$, satisfies the relations $\xi\equiv 1$, mod $\mathfrak{Q}_j$, $j=1, 2, \ldots, s$, $i\neq j$, while no restriction is made concerning the congruence taken modulo $\mathfrak{Q}_i$. If A is any element of $\mathfrak{A}$ it follows at once from the proof used in the third section of the reference K that there exists one and only one simple element A_i in $\mathfrak{A}$ satisfying the relations

$$A_i\equiv A,\ \text{mod}\ \mathfrak{Q}_i,\quad A_i\equiv 1,\ \text{mod}\ \mathfrak{Q}_j,\qquad j=1, 2, \ldots, s;\ i\neq j.$$

Hence the product $A_1A_2\ldots A_s$ is congruent to A modulo every simple factor of $\mathfrak{M}$ and therefore modulo $\mathfrak{M}$. Hence $A=A_1A_2\ldots A_s$ in $\mathfrak{A}$. From the theory of residue classes we also see that this factorization into simple elements is uniquely determined. Hence we have:

THEOREM: *Every element of a finite algebra* $\mathfrak{A}$ *can be uniquely represented as a product of simple elements.*

We shall represent the factorization of A into simple factors by the notation $A=A_1A_2\ldots A_s$. If A is a simple element A_i of type i we may write $1_11_2\ldots 1_{i-1}A_i1_{i+1}\ldots 1_s$, where $1_i=1$ for all values of i. By 0_i we understand an element in $\mathfrak{A}$ that is congruent to 0, mod $\mathfrak{Q}_i$, and congruent to 1, mod $\mathfrak{Q}_j$, $j=1, 2, \ldots, s$, $i\neq j$. Although $1_i=1$, $0_i\neq 0$. Evidently we have

$$1=1_11_2\ldots 1_s\ \text{and}\ 0=0_10_2\ldots 0_s.‡$$

* E. H. Moore, *Bulletin New York Mathematical Society*, Vol. III (1893), p. 75; L. E. Dickson, "Linear Groups," Teubner, 1901.

† K, p. 433.

‡ The results of this section should be compared with Hensel, "Zahlentheorie," pp. 86–92.

We shall define two non-unit elements A and B as *relatively prime* in $\mathfrak{A}$ if there exist two other elements C and D such that $AC+BD=1$. Suppose $A=A_1A_2\ldots.A_i\ldots.A_s$ when written as a product of simple factors. Choose $C=C_1C_2\ldots.C_i\ldots.C_s$ so that $C_i=0_i$ whenever $(A_i, \mathfrak{Q}_i)\neq(1)$, and $A_iC_i=1$ whenever $(A_i, \mathfrak{Q}_i)=(1)$. It has previously been proved that in the latter case the relation $A_iC_i=1$ is always possible.* Evidently we have $A_i0_i=0_i$. Choose $D=D_1D_2\ldots.D_i\ldots.D_s$ so that $D_i=0_i$ whenever $A_iC_i=1$. This includes all cases where $(B_i, \mathfrak{Q}_i)\neq(1)$, for otherwise the residue classes corresponding to both A and B are congruent to 0 modulo the absolute prime modular system contained in $\mathfrak{Q}_i$, and this would preclude any relation of the form $AC+BD=1$ in $\mathfrak{A}$. For all other values of i let $B_iD_i=1$. We see at once that when C and D are so chosen we have $AC+BD\equiv1$, mod $\mathfrak{Q}_i$, $i=1, 2, \ldots., s$, one term always being congruent to 1, the other to 0. Hence, we see from the first theorem of this section that $AC+BD=1$. Hence:

THEOREM: *When two elements A and B of $\mathfrak{A}$ are relatively prime there exist two elements C and D such that $AC+BD=1$, where C always satisfies one of the relations $(C, \mathfrak{Q}_i)=(1)$ or $(C, \mathfrak{Q}_i)=\mathfrak{Q}_i$, $i=1, 2, \ldots., s$, and the same is true of D.*

The expression $A_1\ldots.A_i\ldots.A_s$ is the standard multiplicative form of A. Fraenkel obtained an analogous result but his proof is no longer valid for our more general case.† We shall now proceed to obtain a standard additive form. By a *component* element of type i, written A'_i, we understand an element of $\mathfrak{A}$ such that $A'_i\equiv0$, mod $\mathfrak{Q}_j$, $j=1, 2, \ldots., s$, $i\neq j$, with no restriction upon the case of $\mathfrak{Q}_i$. The standard additive form of an element A in $\mathfrak{A}$ is given by the sum of its components, *i. e.*, $A=A'_1+A'_2+\ldots.+A'_i+\ldots.+A'_s$. A component of type i written in factor form gives the expression

$$A'_i=0_10_2\ldots.0_{i-1}A_i0_{i+1}\ldots.0_s.$$

Hence $A\equiv A'_i$, mod $\mathfrak{Q}_i$, $i=1, 2, \ldots., s$, and our standard additive form is seen to be unique. Hence:

THEOREM: *Every element in $\mathfrak{A}$ is uniquely determined by the sum of its components.*

We see that $A_i\equiv A'_i$, mod $\mathfrak{Q}_i$, but $A_i\equiv1$, and $A'_i\equiv0$, mod $\mathfrak{Q}_j$, $j=1, 2, \ldots., s$, $i\neq j$. Again it is evident that the *i-th* component of $A+B$ is $A'_i+B'_i$. In the product AB we have $A'_iB'_j=0$, $i\neq j$, for this product is congruent to zero modulo every $\mathfrak{Q}_i$. Therefore we have:

THEOREM: *The i-th component of the sum or product of two elements of $\mathfrak{A}$ is equal to the sum or product of the i-th components of the two elements.*

* K, pp. 423–424.

† Fraenkel, *loc. cit.*, p. 166. See also Hensel, "Zahlentheorie," p. 89.

From the preceding theorems we see that if

$$A=A_1A_2\ldots.A_i\ldots.A_s=A'_1+\ldots.+A'_i+\ldots.+A'_s,$$

and

$$B=B_1B_2\ldots.B_i\ldots.B_s=B'_1+\ldots.+B'_i+\ldots.+B'_s,$$

then

$$AB=A_1B_1\ldots.A_iB_i\ldots.A_sB_s=A'_1B'_1+\ldots.+A'_iB'_i+\ldots.+A'_sB'_s.$$

From these considerations it follows that if we write the elements of $\mathfrak{A}$ as sums of their components we have a finite linear algebra with s units E_i, where $E_i=0_1\ldots.0_{i-1}1_i0_{i+1}\ldots.0_s$, such that every element of $\mathfrak{A}$ is of the form $K_1E_1+\ldots.+K_iE_i+\ldots.+K_sE_s$. Here K_i ranges over a set of values simply isomorphic with the set of elements of the algebra $\mathfrak{A}_i$ represented by the residue classes of the modular system $\mathfrak{Q}_i$.* In performing the operations of addition and multiplication we can use the components of type i in place of the elements K_i for all values of i, for these two sets of elements are simply isomorphic. Enough has been said to show that $\mathfrak{A}$ is of the type studied by Dickson,† being equal to the sum of s simple algebras having one unit each, the coefficients of these algebras running over different ranges.

III. *Other Properties of* $\mathfrak{A}$.

We shall not take up the study of the multiplicative groups formed by the elements of $\mathfrak{A}$ since these were treated in the reference cited to which the reader is referred. Turning to the additive groups we see that in many respects they correspond to the modules in the Dedekind theory. In order to obtain a sufficient condition that a set of elements in $\mathfrak{A}$ form an additive group it is merely necessary to take all elements A of $\mathfrak{A}$ that are congruent to zero modulo any system $\mathfrak{M}'$ contained in $\mathfrak{M}$. That this condition is not necessary we see from the group formed by 0 and 1 modulo $(x^2, 2)$. We have, however, the following

THEOREM: *A necessary and sufficient condition that a set of elements in* $\mathfrak{A}$ *form an additive group* G *is that all components of type* i, $i=1, 2, \ldots., s$, *found among the elements of the set form a group* G_i *and that there exists no element of* $\mathfrak{A}$ *not in the set whose i-th component is in* G_i *for all values of* i. *The group* G *is equal to the direct product of the groups* $G_1, G_2, \ldots., G_s$.

To prove that the condition is necessary take the group G' formed by all elements of $\mathfrak{A}$. We know all elements of $\mathfrak{A}$ are obtained if in the expression

$$A=A'_1+A'_2+\ldots.+A'_i+\ldots.+A'_s$$

each of the components A'_i, $i=1, 2, \ldots., s$, ranges unrestrictedly over all

[*] Fraenkel, *loc. cit.*, p. 175.

[†] L. E. Dickson, *Transactions of the American Mathematical Society,* Vol. VI (1905), pp. 344 ff.

values of its set, independent of the others. From this it necessarily follows that G' is the direct product of the s additive groups H_i each of which is composed of all the components of the type designated by the subscript. Since any additive group G of $\mathfrak{A}$ is a subgroup of G' it follows from the theory of groups that G is the direct product of s groups G_i, each G_i being that subgroup of its corresponding H_i that is formed by all components of the type indicated by the subscripts that are found in the elements of G. It is also clear that there exists no element in $\mathfrak{A}$ but not in G all of whose components are in the various G_i, for in forming G as the direct product of the G_i we evidently get an element in G that has exactly this same set of components. This establishes the necessary condition.

To obtain the sufficient condition let us recall that if A and B are two elements of $\mathfrak{A}$ in the set under consideration, and if A'_i and B'_i are their components of type i, then $A+B$ has $A'_i+B'_i$ as its component of type i. Since A'_i and B'_i are in G_i, $i=1, 2, \ldots, s$, the same holds for $A'_i+B'_i$. Therefore it follows from the conditions assumed that $A+B$ must belong to the set. That this set forms a group follows at once for when we add one member of the set to all elements of the set we get back all elements. This proves the theorem.

The multiplication group G formed by the units of $\mathfrak{A}$* furnishes us with an analogue to Dirichlet's general theorem on the units of an algebraic realm, a set of independent generators of the abelian group G corresponding to the linearly independent units of Dirichlet's theorem. To each U corresponds its inverse (or reciprocal) U^{-1} such that $UU^{-1}=1$. Hence the reciprocal of a unit is also a unit. Non-units do not have reciprocals for they are divisors of zero.

We now proceed to define a *prime* element in $\mathfrak{A}$. We say that A is prime in $\mathfrak{A}$ if it cannot be factored into the product of two non-units neither of which is equivalent to A. This is the definition found in the theory of algebraic numbers with an added condition. A non-unit that is not a prime can always be factored into two elements neither of which is a unit. Unless both of these factors are primes this process can be repeated. We shall now show that after a finite number of such steps we can always represent such an element of $\mathfrak{A}$ as a product of primes or powers of primes. Suppose the element has been factored into its simple factors which we now proceed to consider separately. It should be remembered that in the following equivalent elements are regarded as essentially the same. Suppose we proceed to factor the simple element A_i into primes, where A_i naturally is a non-unit, for units are not factored. To do this we must first determine the effect of the above-mentioned additional condition given in the definition of a prime. We see that an element X_i in $\mathfrak{A}$ is defined as a prime even when it factors into two non-units, provided at least

* K, pp. 423–424. See also Vandiver, *loc. cit.*, p. 294.

one factor is equivalent to the element. If U_iX_i is the equivalent factor and $X_i=D_iU_iX_i$, write $D_iU_i=B_i$ and proceed to study the equation $X_i=B_iX_i$, where B_i is a non-unit. Throughout we restrict ourselves to simple elements of type i. If we take the simple modular factor $\mathfrak{Q}_i$ of $\mathfrak{M}$ associated with our simple elements of type i and write down a descending sequence of modular systems as explained on pages 422 and 423 of the reference K previously cited, we see that the only possible solution for X_i is 0_i. For, suppose that $X_i\equiv 0$, mod $\mathfrak{Q}_{i,\tau}$, but not modulo $\mathfrak{Q}_{i,\tau-1}$. Since B_i is a non-unit it therefore follows that $X_iB_i=X_i$ is congruent to zero modulo $\mathfrak{Q}_{i,\tau-1}$, which leads to a contradiction except when $X_i=0_i$, where we may take $\mathfrak{Q}_{i,0}=\mathfrak{Q}_{i,1}=\mathfrak{Q}_i$. If $B_i\neq 0_i$ it follows from the reference just cited that there exists a power of B_i, $B_i^\epsilon\neq 0_i$, such that $B_iB_i^\epsilon=0_i$. Hence in this case 0_i cannot be a prime by definition. This case always occurs except when $\mathfrak{Q}_i$ is an absolute prime modular system, the only case in which there exists no non-unit element of type i outside of 0_i. Hence in this case we have $0_i=0_i^\alpha$, $\alpha=1, 2, \ldots.$, etc., but no other factorization. Therefore our definition of a prime includes

(a) all elements that cannot be factored into two non-unit elements,

(b) the element 0_i whenever the corresponding modular system $\mathfrak{Q}_i$ is an absolute prime system.

Let us now proceed to factor A_i and suppose for the present that $A_i\neq 0_i$. If a finite number of steps is not sufficient to factor this element into a product of primes and their powers it follows that since $\mathfrak{A}$ contains but a finite number of simple elements of type i, that at least one factor must occur to an arbitrarily high power. Denote this factor by C_i. Since $(C_i, \mathfrak{Q}_i)\neq(1)$, there exists by the reference of the preceding paragraph a definite power α of C_i such that $(C_i^\alpha, \mathfrak{Q}_i)=\mathfrak{Q}_i$, which contradicts the fact that C_i^α is a factor of A_i while $A_i\neq 0_i$. Hence a finite number of factorizations is sufficient for this case. If $C_i=0_i$ it follows from the preceding paragraph that we can either write 0_i as the product of two non-units neither of them equal to 0_i, and then proceed$_i$ as before, or we have 0_i equal to a prime by definition. Hence every element of $\mathfrak{A}$ can be written as the product of prime factors. But this factorization is not unique as we see from the example

$$x_2^2\equiv x_2x_2\equiv(x_1+x_2)^2, \quad \text{mod } (x_1^3, x_2^2, 2),$$

where we can easily verify that both x_2 and x_1+x_2 are primes in the algebra defined by $(x_1^3, x_2^2, 2)$. In this respect our algebra differs essentially from the type studied by Fraenkel. Two primes of $\mathfrak{A}$ need not necessarily be relatively prime, a fact that might be expected from the failure of the unique factorization law. In fact this presupposes the condition $AC+BD=1$ which cannot hold in the above example since $A=x_2$ and $B=x_1+x_2$ are both congruent to 0, mod $(x_2, x_1, 2)$, so that the left-hand side of $AC+BD=1$ is congruent to 0, mod $(x_2, x_1, 2)$, while this cannot be true of the right-hand side. It furthermore follows that no two primes of an algebra defined by a simple modular system can be relatively prime. Hence, we have the following

THEOREM: *In the finite algebra corresponding to the modular system* $\mathfrak{M}=\mathfrak{Q}_1\mathfrak{Q}_2\ldots.\mathfrak{Q}_s$ *there exists s and no more than s primes that are relatively prime each to each.*

Any prime in $\mathfrak{A}$ is equivalent to a prime that is also simple. The first α powers of this latter element are distinct elements of $\mathfrak{A}$, but all later ones are equal to the α-th power which is of the form $1_1\ldots.1_{i-1}0_i1_{i+1}\ldots.1_s$. The first prime when raised to powers has its first α powers essentially different, but all following ones are of the form $U_1\ldots.U_{i-1}0_iU_{i+1}\ldots.U_s$, where the various U_j run over subgroups of the group of units. Hence, we get:

THEOREM: *The first α powers of a simple prime in $\mathfrak{A}$ are essentially different, those following are identical with the α-th power which equals* 0_i. *If a prime is not simple its first α powers are essentially different, while all following powers form a repeating cycle of equivalent elements.*

The algebra $\mathfrak{A}$ also contains sub-algebras. Such can be obtained by taking all elements of $\mathfrak{A}$ that have certain components, say the last $s-t$, equal to 0, *i. e.*, in product form these elements can be written $A_1\ldots.A_t0_{t+1}0_{t+2}\ldots.0_s$. The 0 of $\mathfrak{A}$ is always in such a sub-algebra, but this is never true of any unit of $\mathfrak{A}$. We may, however, let $1_1\ldots.1_t0_{t+1}\ldots.0_s$ take the place of 1, and let the units of the sub-algebra be those elements whose first t simple factors are units of $\mathfrak{A}$. This sub-algebra is simply isomorphic to the algebra $\mathfrak{A}'$ corresponding to $\mathfrak{M}'=\mathfrak{Q}_1\mathfrak{Q}_2\ldots.\mathfrak{Q}_t$.[*] Comparing this with a necessary and sufficient condition that a set of elements in $\mathfrak{A}$ form a multiplicative group[†] we have:

THEOREM: *There exists a* (1, 1) *correspondence between* 2^λ *sub-algebras of* $\mathfrak{A}$ *and the* 2^λ *multiplicative groups in* $\mathfrak{A}$ *such that the group corresponding to a given sub-algebra is composed of its units.*

In closing we may ask if it is possible to restore the unique factorization law by means of ideals as in the Dedekind theory. This is not the case. Closer study of the subject shows that in such a theory the analogue of an ideal would be the set of all elements of $\mathfrak{A}$ that are congruent to 0 modulo one of the s absolute prime modular systems that $\mathfrak{M}$ contains. In the example already given, namely $\mathfrak{M}=(x_2^3, x_1^2, 2)$, this would give but one (so-called) ideal, and this would be of no avail in solving the factorization of $x_2^2\equiv x_2x_2\equiv(x_1+x_2)^2$, mod $\mathfrak{M}$, uniquely. We can, however, obtain in this manner a number of results analogous to theorems in the theory of algebraic numbers.

HARVARD UNIVERSITY.

[*] See Hensel, "Zahlentheorie," pp. 78 ff.

[†] See K, p. 428.